

Anti-Terrorism and Supply Chain Security Policy

1. Purpose

- (1) CINCON Electronics, Inc. (the "Company") is committed to protecting the security of its operations, employees, cargo, and supply chain. With reference to the security requirements of the U.S. Customs and Border Protection Customs Trade Partnership Against Terrorism (CTPAT) program, the Company establishes and continuously improves its supply chain security management practices.
- (2) Through risk assessments, personnel and facility security, cargo and transportation controls, business partner management, employee training, incident reporting, and emergency response measures, the Company seeks to reduce risks related to terrorism, unauthorized access, smuggling, cargo tampering, and other supply chain security threats while protecting operational security, cargo integrity, and customer interests.

2. Our Commitments

(1) Operational and Supply Chain Security

The Company maintains appropriate supply chain security management mechanisms and continuously identifies and assesses security risks throughout raw material supply, manufacturing, warehousing, packaging, loading, unloading, and transportation activities and implements appropriate preventive and control measures.

(2) Prevention of Terrorism and Illegal Activities

The Company prohibits the use of its premises, equipment, products, cargo, transportation resources, or supply chain to engage in or facilitate terrorism, smuggling, illegal transportation, cargo tampering, or other unlawful activities.

(3) Cargo and Transportation Security

Based on applicable risks, the Company maintains appropriate controls for cargo, warehousing, loading, unloading, and transportation to reduce the risk of unauthorized persons, materials, or prohibited items entering the cargo and transportation process and to protect cargo integrity.

(4) Personnel and Facility Security

The Company maintains appropriate personnel identification, access control, visitor management, and facility security measures based on operational needs to prevent unauthorized access to controlled areas and reduce risks to personnel and facilities.

(5) Business Partner Security Management

Based on supply chain risks and business needs, the Company appropriately assesses and manages suppliers, logistics providers, contractors, and other business partners and encourages relevant partners to maintain supply chain security measures appropriate to their operations and risk exposure.

(6) Security Awareness

Through training, internal communications, and appropriate management measures, the Company enhances employees' awareness and capabilities relating to anti-terrorism, supply chain security, identification of suspicious activities, incident reporting, and emergency response.

3. Risk Management and Preventive Measures

To reduce terrorism and other supply chain security risks, the Company implements appropriate measures based on its operations and risk exposure, including:

- (1) Conducting periodic or risk-based supply chain security assessments to evaluate the effectiveness and suitability of relevant security measures.
- (2) Maintaining appropriate security controls for facilities, warehouses, access points, visitors, and other controlled areas.

- (3) Managing cargo receiving, storage, packaging, loading, shipping, and transportation processes to protect cargo security and integrity.
- (4) Providing necessary security training and awareness programs for personnel involved in supply chain activities.
- (5) Assessing or verifying the security practices of relevant supply chain partners as appropriate based on risk and business needs.
- (6) Periodically reviewing this Policy and related security measures and implementing improvements in response to changing risks and applicable requirements.

4. Incident Reporting and Emergency Response

- (1) Employees who become aware of or reasonably suspect terrorist activity, unauthorized access, smuggling, suspicious persons or items, cargo tampering, transportation security incidents, or other circumstances that may threaten the security of the Company or its supply chain should promptly report the matter through the Company's designated reporting channels.
- (2) Upon receiving a report, the Company will take appropriate verification, control, and emergency response measures based on the nature of the incident. Significant security incidents or suspected unlawful activities will be reported to the appropriate authorities or handled with other necessary assistance in accordance with applicable laws and regulations.

5. Reporting Protection and Incident Handling

- (1) **Information for Investigation**
Reporting persons should, where reasonably possible, provide specific information sufficient to assist the Company in reviewing and responding to the reported matter.
- (2) **Confidentiality and Prohibition of Retaliation**
The Company will appropriately protect the identity and related information of persons making good-faith reports to the extent permitted by applicable law and necessary for the investigation. Retaliation or other adverse treatment against such persons is prohibited.
- (3) **Handling of Violations**
Where an investigation confirms a violation of this Policy, Company requirements, or applicable laws and regulations, the Company will take appropriate corrective and remedial measures based on the circumstances. Unlawful conduct will be handled in accordance with applicable law.

6. Reporting Channels

Contact Department: Administration Department

Hotline: +886-4-769-0261, Ext. 110

Email: hr@cincon.com.tw

7. Continuous Improvement

The Company will continue to monitor developments in applicable supply chain security requirements, CTPAT security criteria, and international supply chain risks. This Policy and related management measures will be periodically reviewed and updated as appropriate based on operational needs and changes in risk to continuously enhance the security and resilience of the Company's supply chain.